PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

BEST PRACTICES FOR ISS RISK MANAGEMENT

Using the Results of the EBIOS® Method in a BS 7799 Process

21 March 2003 version

51 bd de La Tour-Maubourg - 75700 PARIS 07 SP - Tel +33(0)1 71 75 84 15 - Fax +33(0)1 71 75 84 00

What is BS 7799?

British Standard 7799 (BS 7799) comprises two guides: ISO/IEC 17799:2000 and BS 7799-2:2002.
ISO/IEC 17799:2000 is a catalogue listing 36 control objectives, which are divided into 127 controls covering 10 different areas (security policy, employee security, access control, etc.). The control objectives describe a goal and what must be done to achieve that goal. They are then subdivided into controls, with explanations (in varying degrees of detail) of what must be done in order to implement them.
BS 7799-2:2002 describes an Information Security Management System (ISMS) based on four recurrent steps (Plan, Do, Check, Act) similar to those described in the quality standards ISO 9001 and ISO 14001. Use of ISO/IEC 17799:2000 is recommended at the planning stage.

What benefits does the EBIOS method offer as part of a BS 7799 process?

Conducting an EBIOS study upstream of the BS 7799 process offers several benefits:

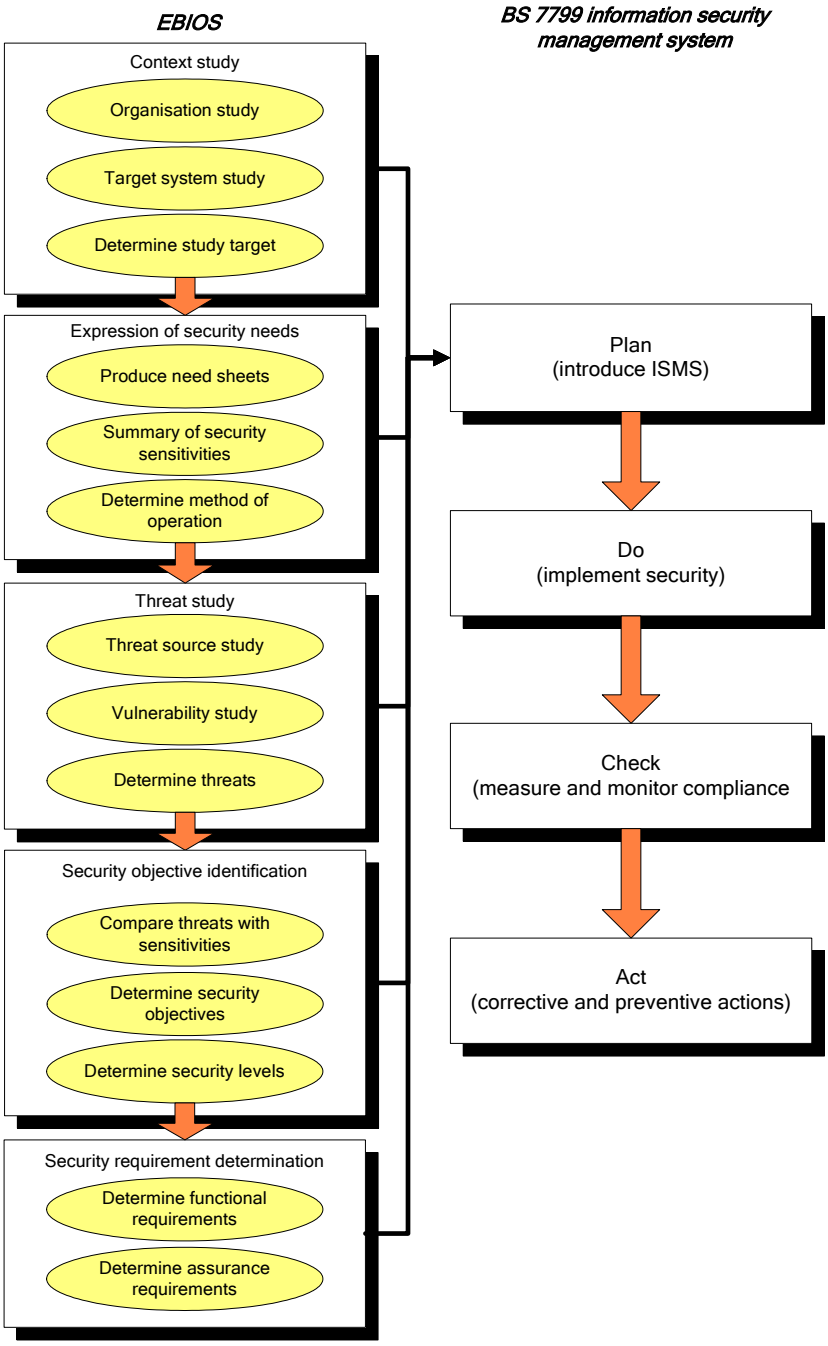
- Rationale for the choice of objectives and controls from the catalogue, based on the organisation's actual needs,
- Compliance with the process framework described in BS 7799, which advocates assessing the risks before selecting objectives and controls,
- The study provides reusable results (relating to the context, security sensitivities, threats, risks, security objectives and security requirements) that will be available for subsequent iterations of the information security management system.

How is EBIOS used in a BS 7799 process?

One effective solution for implementing a BS 7799 strategy consists in:

- Formally specifying the scope of the information security management system,
- Preparing a security policy,
- Conducting a global EBIOS study in order to analyse, evaluate and process the risks, selecting objectives and controls that cover the risks that must be reduced,
- Preparing a statement of applicability,
- Conducting the rest of the process using other tools.

The following data can be used for this purpose:



(For more information, please contact: ebios.dcssi@sgdn.pm.gouv.fr)